Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2025-08-28

Generated by Acunetix

Scan of ap.tnnua.edu.tw

Scan details

Scan information	
Start time	2025-08-28T17:00:00.933537+08:00
Start url	https://ap.tnnua.edu.tw/OrdSupp2018/Default2018.aspx
Host	ap.tnnua.edu.tw
Scan time	16 minutes, 38 seconds
Profile	Full Scan
Responsive	True
Server OS	Windows
Server technologies	ASP.NET,ASP.NET
Application build	25.4.250417124

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	7
Critical	0
High	1
Medium	1
Low	0
Informational	5

Alerts summary

Insecure Transportation Security Protocol Supported (TLS 1.0)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N Base Score: 6.3 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-326

Affected items	Variation
Web Server	1

TLS/SSL Weak Cipher Suites

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 3.3 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310

Affected items	Variation
Web Server	1

An Unsafe Content Security Policy (CSP) Directive in Use

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

default-src Used in Content Security Policy (CSP)

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

Insecure Transportation Security Protocol Supported (TLS 1.1)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:N/SA:N Base Score: 6.3 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-326

Affected items	Variation
Web Server	1

Outdated JavaScript libraries

Classification

CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-937

Affected items	Variation
Web Server	1

Permissions-Policy header not implemented

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Alerts details

Insecure Transportation Security Protocol Supported (TLS 1.0)

Severity	**High**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.0.
Request headers

TLS/SSL Weak Cipher Suites

Severity	**Medium**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The remote host supports TLS/SSL cipher suites with weak or insecure properties.

Impact

Recommendation

Reconfigure the affected application to avoid use of weak cipher suites.

References

OWASP: TLS Cipher String Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)
OWASP: Transport Layer Protection Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)
Mozilla: TLS Cipher Suite Recommendations (https://wiki.mozilla.org/Security/Server_Side_TLS)
SSLlabs: SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2 (https://datatracker.ietf.org/doc/html/rfc9155)

Affected items

Web Server
Details
Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 443): • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA Weak TLS/SSL Cipher Suites: (offered via TLS1.1 on port 443): • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443): • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA
Request headers

An Unsafe Content Security Policy (CSP) Directive in Use

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **An Unsafe Content Security Policy (CSP) Directive in Use**
  - **First observed on:** https://ap.tnnua.edu.tw/OrdSupp2018/
  - **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-src 'self'; frame-ancestors 'self';
  - **CSP Source:** header
  - **Summary:** Acunetix detected that one of following CSP directives is used: unsafe-eval, unsafe-inline. By using unsafe-eval, you allow the use of string evaluation functions like eval. By using unsafe-inline, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.
  - **Remediation:** If possible remove unsafe-eval and unsafe-inline from your CSP directives.
  - **References:**
    - N/A

Request headers

```
GET /OrdSupp2018/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/OrdSupp2018/

Cookie: ASP.NET_SessionId=rmbljj2oaj0elwu2nyypnt5q

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive
```

default-src Used in Content Security Policy (CSP)

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **default-src Used in Content Security Policy (CSP)**
  - **First observed on:** https://ap.tnnua.edu.tw/OrdSupp2018/
  - **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; frame-src 'self'; frame-ancestors 'self';
  - **CSP Source:** header
  - **Summary:** Acunetix detected that you used default-src in CSP directive. It is important to know that default-src cannot be used as a fallback for the functions below: base-uri, form-action, frame-ancestors, plugin-types, report-uri, sandbox
  - **Impact:** N/A
  - **Remediation:** N/A
  - **References:**
    - N/A

Request headers

```
GET /OrdSupp2018/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/OrdSupp2018/

Cookie: ASP.NET_SessionId=rmbljj2oaj0elwu2nyypnt5q

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive
```

Insecure Transportation Security Protocol Supported (TLS 1.1)

Severity	**Informational**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1 (https://tools.ietf.org/html/rfc8996)
Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)
PCI 3.1 and TLS 1.2 (Cloudflare Support) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.1.
Request headers

Outdated JavaScript libraries

Severity	**Informational**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

References

How Invicti identifies Out-of-date technologies (https://www.invicti.com/support/how-invicti-identifies-outofdate/)

Affected items

Web Server
Details
• **jQuery 3.5.1** ◦ URL: https://ap.tnnua.edu.tw/OrdSupp2018/Default2018.aspx ◦ Detection method: The library's name and version were determined based on its dynamic behavior. ◦ References: ▪ https://code.jquery.com/
Request headers

```
GET /OrdSupp2018/Default2018.aspx HTTP/1.1

Referer: https://ap.tnnua.edu.tw/OrdSupp2018/Default2018.aspx

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive
```

Permissions-Policy header not implemented

Severity	**Informational**
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server
Details

Locations without Permissions-Policy header:

- https://ap.tnnua.edu.tw/OrdSupp2018/Default2018.aspx
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/fonts/DejaVu/
- https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/cultures/kendo.culture.zh-TW.min.js
- https://ap.tnnua.edu.tw/OrdSupp2018/WebResource.axd
- https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/messages/kendo.messages.zh-TW.min.js
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Images/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/fonts/glyphs/
- https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/
- https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/jquery-migrate-3.3.2.min.js
- https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/cultures/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/
- https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/messages/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/TypIcons/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/textures/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/Default/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/Images/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/fonts/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/kendo.silver.min.css
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/Silver/
- https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/style.css

Request headers

```
GET /OrdSupp2018/Default2018.aspx HTTP/1.1

Referer: https://ap.tnnua.edu.tw/OrdSupp2018/Default2018.aspx

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive
```

Scanned items (coverage report)

https://ap.tnnua.edu.tw/
https://ap.tnnua.edu.tw/OrdSupp2018/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Images/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Images/16/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/kendo.ext.css
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/Default/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/fonts/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/fonts/DejaVu/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/fonts/glyphs/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/Images/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/kendo.common.min.css
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/kendo.default.min.css
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/kendo.silver.min.css
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/Silver/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/style.css
https://ap.tnnua.edu.tw/OrdSupp2018/Content/Styles/textures/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/TypIcons/
https://ap.tnnua.edu.tw/OrdSupp2018/Content/TypIcons/typicons.min.css
https://ap.tnnua.edu.tw/OrdSupp2018/Default2018.aspx
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/cultures/
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/cultures/kendo.culture.zh-TW.min.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/jquery-3.5.1.min.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/jquery-migrate-3.3.2.min.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/jquery.myUtil.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/kendo.web.ext.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/kendo.web.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/kendo.zh-TW.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/lodash.min.js
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/messages/
https://ap.tnnua.edu.tw/OrdSupp2018/Scripts/messages/kendo.messages.zh-TW.min.js
https://ap.tnnua.edu.tw/OrdSupp2018/WebResource.axd